User Guide for Paros v2.x

Table of Contents

1 Introduction

"Paros" was written completely in Java by people from ProofSecure.com. It is for people who need to evaluate the security of their web applications. Through Paros's proxy nature, all HTTP and HTTPS data between server and client, including cookies and form fields, can be intercepted and modified.

This user guide is to help people familiar with the Paros functionalities and the GUI interface.

1.1 Paros Overview

Paros is a HTTP/HTTPS proxy for assessing web application vulnerability. It supports editing/viewing HTTP messages on−the−fly with client−certificate, proxy−chaining, filtering and intelligent vulnerability scanning.

Running Platform:

- platform independent but required JRE 1.4.x to be installed.

1.2 History

Paros v1.0 first released in Aug 2002:

- allows people to intercept both HTTP and HTTPS requests/responses

Paros v2.0 released in Dec 2002:

- GUI interface completely rewritten
- A tree view showing the website hierarchy
- Core proxy engine rewritten
- Scanner feature added
- Filter feature added

Paros v2.1 released on 24 Apr 2003:

- Support client certificate
- Scanner engine improved
- A few vulnerability checks added
- Filters added to record GET/POST queries
- Hash function and base64 conversion added

Paros v2.2 released on 30 Jun 2003:

- Support HTTP 1.1 connections
- Spider feature added
- Allow to scan for cross−site scripting (XSS) vulnerability on the selected website after navigation.
- Allow removal of websites from the Tree view

2 Copyright

“Paros” proxy is Copyright 2002 – 2003 by ProofSecure.com. This program is freeware under the license stated in Appendix I. Basically, this program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. Read “Appendix I – Freeware License” for further details.

3 Installation

1. Ensure Java Run Time Enviroment (JRE) 1.4 (or above) was installed. If not, goto http://java.sun.com/j2se to download and install it.

2. Download the Paros program file from our website.

3. For Windows version, just follow the instructions in the setup program. Shortcuts will then be created. Click the desktop shortcut to run the program.

4. For Unix or other plateforms, unzip all the files in a new directory manually. Click the .jar file to run the program.

5. Paros uses two ports. *Port 8080 for proxy connection and port 8443 for internal SSL handling. So, make sure these two ports are not in use by other applications*. You can change the ports and other settings in the "Options" tab of the program.

6. Open web browser such as IE, configure the proxy with proxy name "localhost" and proxy port "8080" for both HTTP and HTTPS. Note that port 8443 is used by Paros itself, and not for the use of web browser.

7. If your PC is running behind firewall and can only access Internet through a pre−defined company proxy, you need to modify the proxy setting in Paros. Just click the tab "Options" tab and modify the two fields "ProxyName" and "ProxyPort".

4 Configuration

1. Start the program.
2. Check if error message is shown during initialization. Usually, initialization error occurs when port 8080 and 8443 are being used by other programs or web servers.
3. Goto “Options” tab and you can see:

```
<?xml version="1.0" encoding="utf−8" ?>

<Options xmlns="http://tempuri.org/XMLSchemaOptions.xsd">

        <ProxyServer>

                <!−− IP address of this proxy.  Use localhost or
127.0.0.1 −−>

                <IP>127.0.0.1</IP>

                <!−−         Proxy port of listen by this proxy.
Config browser to

                        point to this −−>

                <Port>8080</Port>

                <!−− internal SSL proxy port used by this proxy
−−>

                <SSL>8443</SSL>

        </ProxyServer>

        <ProxyChain>

                <!−− Use blank "Name" if no proxy chain to use
−−>

                <Name></Name>

                <Port>8080</Port>

                <Skip></Skip>

        </ProxyChain>

</Options>
```

4. Modify the above parameters according to your PC environment. For example, if you want other workstations to access web servers via your Paros proxy, you need to set the <IP> to your network IP address (say, 192.168.0.1) rather than 127.0.0.1. Setting the <IP> to 127.0.0.1 will only allow the localhost to use Paros proxy.

```
<ProxyChain>

        <!−− Use blank "Name" if no proxy chain to use −−>

        <Name>proxy.company.com</Name>

        <Port>8080</Port>

        <Skip>192.168.*</Skip>

</ProxyChain>
```

5. Another example is that, if you need to access Internet via a default company proxy (say, proxy.company.com), you can set the <Name> in <ProxyChain> as above. Also, with the above configuration, Paros proxy will connect to Internet via your company proxy, and at the same time, connect directly to web servers with IP addresses 192.168.0.* as stated in the <Skip> parameter.

6. After configuration, click the “Save” button in the “Options” tab to save the modification. Paros proxy will then be re−initialized to make your configuration effective.
7. You can now try to use web browser to access website via Paros.

***Remember* that, for all verisons of Paros, whenever you try to access SSL website via Paros, a certificate warning would be shown on the browser. This is because Paros acts as a man−in−the−middle and need to use its own certificate to decrypt the messages. In order to continue, you must accept the certificate (or just import it to suppress this warning).**

5 Functions

5.1 Spider

Spider is used to crawl the websites and gather as many URL links as possible. This allows you to have a better understanding of the web site hierarchy tree in a short time before mnual navigation.

Currently, the “Spider” function is in beta version. Its functionalities include:

- Crawl HTTP and HTTPS websites based on given URL, e.g. http://www.abc.com or https://www.abc.com
- Support cookie
- Support proxy chaining, which is set at the <ProxyChain> field in Option tab (but setting the <Skip> field has not effect on the spider)
- Automatically add URL links to the web site hierarchy tree for later scanning.

As it is just a simple spider, it has the following limitations:

- SSL websites with invalid certificate cannot be crawled
- Muti−threading not supported
- Some ‘malformed’ URLs in HTML pages cannot be recognized

Also, URLs generated by Javascript cannot be found using this spider. Those URLs, however, can be found and added to the hierarchy tree through manual navigation.

5.2 Scanner

The scanner function is to scan the server based on the website hierarchy (the tree on the left panel). It can check if there is any server misconfiguration.

We added this functionality in Paros because we found that certain URL paths cannot be found and examined by the crawler engine of web scanners automatically. For example, some URL links can only be shown after valid logon. Automatic web scanner may not be able to find out the paths and check if there exists any backup files (.bak) which could expose server information.

In order to use this function, you need to navigate the website first. After you logon a website and navigate it, a website hierarchy tree will be built by Paros automatically. Then you can do the following things:

- If you want to scan all websites on the tree, you can then click on the menu item "Tree" => "Scan All" to trigger the scanning.
- If you just want to scan one website on the tree, you can click on that site in the tree panel and click menu item "Tree" => "Scan selected Node" (You can also right−click on the tree view and choose the options).

Currently, Paros has the following checks:

- HTTP PUT allowed − check if the PUT option is enabled at server directories
- Directory indexable − check if the server directories can be browsable.
- Obsolete files existed − check if there exists obsolete files at

- Cross−site scripting − check if cross−site scripting (XSS) is allowed on the query parameters
- Default files on websphere server – check if default files existed on websphere server

Note that all the above checks are based on the URLs in the website hierarchy. That means the scanner will check each URL for each vulnerability. Compared with other web scanners which just do a blink scan without website hierarchy, our scanning result is more accurate.

5.3 Filter

The use of filters is to:

- Detect and alert you the occurrence of certain pre−defined patterns in HTTP message. So, you do not need to trap every HTTP message and seek for the pattern you want.
- Log information in which you are interested, for example, cookies.

As filters intercept and examine each HTTP(S) message on the fly, enabling all the filters could slow down the proxy speed. So, we recommended to only turn on those filters you need (by default, only the LogCookie filter is enabled after start).

Currently, Paros has the following filters:

- LogCookie
    - log all the accepted cookies sent from browser to server on the lower panel.
- LogGetQuery
    - log all the HTTP(S) GET queries sent from browser. The log named ‘get.xls’ will be saved in the Paros program directory.
- LogPostQuery
    - log all the HTTP(S) POST queries sent from browser. The log named ‘post.xls’ will be saved in the Paros program directory.
- CookieDetectFilter
    - Alert you the "Set−Cookie" attempt in HTTP response and allow you to modify it.
- IfModifiedSinceFilter
    - remove 'If−Modified−Since' & 'If−None−Match' header fields in HTTP request. This can be used to retrieve ‘HTTP 200 OK’ response instead of ‘HTTP 304 not modified’.

5.4 Trapping HTTP requests and responses

Paros can trap and modify HTTP(and HTTPS) requests/responses manually. All the HTTP and HTTPS data passing through Paros can be trapped and modified as you like.

1. Trap Request

Just turn on the "Trap Request" check box in the "Trap" tab and all requests will then be trapped. You can modify the content in the Header/Body text area and click "Continue" button to proceed.

Note that there is a button "Tabular View" at the right bottom corner. This button can only be used when the check box "Trap Request" is on and there is some text in the "Body" text area. It is used to convert the HTTP POST query to table form for your easy editing. After modified the parameters, you can just click the "Original View" button and go back to the previous screen with the updated query.

2. Trap Response

Turn on the "Trap Response" check box in the "Trap" tab and all response will then be trapped. You can modify the content in the Header/Body text area and click "Continue" button to proceed.

Note that the "Tabular View" button here is useless. It is only useful when trapping HTTP(S) POST requests.

5.5 Other Functions

Besides the main functions, there are some other features in Paros:

o Support client certificate – some web applications require client certificate. Many man−in−the−middle proxies cannot work under this situation because they could not store the client certificate for handshaking or logon. By importing the required client certificate into Paros just before handshaking or logon, you can intercept and modify HTTP data with those web applications which require client certificate. To use this feature, you can click Menu => Tools => Enable Client Cert.

o Log HTTP requests and responses on−the−fly. The response time is also logged.

o Convert data into different encoding/hash formats including Base64, SHA1 and MD5 (Menu => Tools => Hash/Encoding).

6 Appendix I – Freeware License

PAROS FREE EDITION END USER LICENSE AGREEMENT

IMPORTANT: THIS SOFTWARE END USER LICENSE AGREEMENT ("EULA") IS A LEGAL AGREEMENT BETWEEN YOU AND THE AUTHOR. READ IT CAREFULLY BEFORE COMPLETING THE INSTALLATION PROCESS AND USING THE SOFTWARE. IT PROVIDES A LICENSE TO USE THE SOFTWARE AND CONTAINS WARRANTY INFORMATION AND LIABILITY DISCLAIMERS. BY OPENING THE SOFTWARE, YOU ARE CONFIRMING YOUR ACCEPTANCE OF THE SOFTWARE AND AGREEING TO BECOME BOUND BY THE TERMS OF

THIS AGREEMENT. YOU AGREE TO THE TERMS OF THIS AGREEMENT. IF YOU ARE ACCESSING THE SOFTWARE ELECTRONICALLY, INDICATE YOUR ACCEPTANCE OF THESE TERMS BY SELECTING THE "ACCEPT" BUTTON AT THE END OF THIS AGREEMENT.

IF YOU DO NOT AGREE TO ALL THESE TERMS, PROMPTLY RETURN THE UNUSED SOFTWARE TO YOUR PLACE OF PURCHASE FOR A REFUND OR, IF THE SOFTWARE IS ACCESSED ELECTRONICALLY, SELECT THE "DECLINE" BUTTON AT THE END OF THIS AGREEMENT.

Section 1. Definitions

(a) "Author" means the author of the software from ProofSecure.com.

(b) "Software" means the software supplied by the Author herewith, which may also include documentation, associated media, printed materials, and online and electronic documentation.

Section 2. License

This EULA allows you to:

(a) Install and use the Software on a single computer; OR install and store the Software on a storage device, such as a network server, used only to install the Software on your other computers over an internal network, provided you have a license for each separate computer on which the Software is installed and run. A license for the Software may not be shared or used concurrently on different computers.

(b) Make one copy of the Software in machine−readable form solely for backup purposes. You must reproduce on any such copy all copyright notices and any other proprietary legends on the original copy of the Software.

Section 3. License Restrictions

(a) Other than as set forth in Section 2, you may not make or distribute copies of the Software, or electronically transfer the Software from one computer to another or over a network.

(b) You may not decompile, reverse engineer, disassemble, or otherwisereduce the Software to a human−perceivable form.

(c) You may not rent, lease, or sublicense the Software.

(d) You may permanently transfer all of your rights under this EULA only as part of a sale or transfer, provided you retain no copies, you transfer all of the Software (including all component parts, the media and printed materials, any upgrades, this EULA, and the serial numbers if applicable), and the recipient agrees to the terms of this EULA. If the Software is an upgrade, any transfer must include all prior versions of the Software. You may not sell or transfer any Software purchased under a volume discount.

(e) You may not modify the Software or create derivative works based upon the Software.

(f) You may not export the Software into any country prohibited by the Hong Kong SAR regulations thereunder.

(g) In the event that you fail to comply with this EULA, the Author may terminate the license and you must destroy all copies of the Software.

(h) You agree to make reasonable efforts to control and prevent the software to be used other than the expected personnel.

Section 4. Upgrades

If this copy of the Software is an upgrade from an earlier version of the Software, it is provided to you on a license exchange basis. You agree by your installation and use of this copy of the Software to voluntarily terminate your earlier EULA and that you will not continue

to use the earlier version of the Software or transfer it to another person or entity unless such transfer is pursuant to Section 3.

Section 5. Ownership

The foregoing license gives you limited license to use the Software. The Author and the software suppliers retain all right, title and interest, including all copyrights, in and to the Software and all copies thereof. All rights not specifically granted in this EULA,

including Copyrights, are reserved by the Author and the software suppliers.

Section 6. NO WARRANTY. The Software is being delivered to you "AS IS" and the Author makes no warranty as to its use or performance. THE AUTHOR AND ITS SUPPLIERS DO NOT AND CANNOT WARRANT THE PERFORMANCE

OR RESULTS YOU MAY OBTAIN BY USING THE SOFTWARE. EXCEPT FOR ANY WARRANTY, CONDITION, REPRESENTATION OR TERM TO THE EXTENT TO WHICH THE SAME CANNOT OR MAY NOT BE EXCLUDED OR LIMITED BY LAW APPLICABLE TO YOU IN YOUR JURISDICTION, PROOFSECURE AND ITS SUPPLIERS MAKE NO WARRANTIES CONDITIONS, REPRESENTATIONS, OR TERMS (EXPRESS OR IMPLIED WHETHER BY STATUTE, COMMON LAW, CUSTOM, USAGE OR OTHERWISE) AS TO ANY MATTER INCLUDING WITHOUT LIMITATION NONINFRINGEMENT OF THIRD PARTY RIGHTS, MERCHANTABILITY, INTEGRATION, SATISFACTORY QUALITY, OR FITNESS FOR ANY PARTICULAR PURPOSE.

Section 7. LIMITATION OF LIABILITY

(a) NEITHER THE AUTHOR NOR THE SOFTWARE SUPPLIERS SHALL BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUDING DAMAGES FOR LOSS OF BUSINESS, LOSS OF PROFITS, BUSINESS, INTERRUPTION OR THE LIKE), ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE OR THIS EULA BASED ON ANY THEORY OF LIABILITY INCLUDING BREACH OF CONTRACT, BREACH OF WARRANTY, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY OR OTHERWISE, EVEN IF THE AUTHOR OR ITS REPRESENTATIVES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES AND EVEN IF A REMEDY SET FORTH HEREIN IS FOUND TO HAVE

FAILED OF ITS ESSENTIAL PURPOSE.

(b) THE LIABILITY TO YOU FOR ACTUAL DAMAGES FOR ANY CAUSE WHATSOEVER WILL BE LIMITED TO THE AMOUNT PAID BY YOU FOR THE SOFTWARE THAT CAUSED SUCH DAMAGE.

(c) IN NO EVENT WILL THE AUTHOR BE LIABLE TO ANY DAMAGES ON THIRD

PARTIES DUE TO THE USE OF THIS SOFTWARE BY THE END USER.

Section 8. Basis of Bargain

The Limited Warranty, Exclusive Remedies and Limited Liability set forth above are fundamental elements of the basis of the agreement between the Author and you. The Author would not be able to provide the Software on an economic basis without such limitations.

Section 9. Consumer End Users Only

The limitations or exclusions of warranties and liability contained in this EULA do not affect or prejudice the statutory rights of a consumer, i.e., a person acquiring goods otherwise than in the course of a business.

Section 10. General Provisions

This EULA shall be governed by the laws of the Hong Kong SAR, without giving effect to principles of conflict of laws. This EULA contains the complete agreement between the parties with respect to the subject matter hereof, and supersedes all prior or contemporaneous agreements or understandings, whether oral or written.

Third party trademarks, trade names, product names and logos may be the

trademarks or registered trademarks of their respective owners.